Note: The NAMS module referred to in this document (2.1.a (2), 2.1.e (2), 2.1.g (1), 2.1.g (2)) is currently under construction and is not yet available for use. Users will be informed when the module is available. Until the module is available, please contact your Center CIO for authorization prior to travel, per ITSD memo "Personal Use of Government Office Equipment Including Information Technology: International Travel"

https://inside.nasa.gov/system/files/s3009095315070710040.pdf

Subject: Use of NASA Information and Information Systems while Outside of the U.S. and Territories

Responsible Office: Office of the Chief Information Officer

P.1 Purpose

a. This document establishes requirements and responsibilities for the use and handling of NASA information and information technology (IT) by NASA personnel preparing for, participating in, and returning from travel, work, study or other activities outside of the United States (U.S.) and territories.

b. Use of IT outside of the U.S. and territories creates risks to NASA information, information systems and personnel that are greater than those risks present during work and travel within the United States. For example, the use of mobile devices to transmit or receive information via telecommunication networks makes transmitted information susceptible to eavesdropping, interception and theft. Due to the ease with which entities can monitor transmissions, risks are higher while on international travel in locations where telecommunication networks are owned or controlled by the host government. IT devices are always at risk for the introduction of malicious software, but such risks are greater when devices leave the physical control of the user or when they are connected to networks external to the United States and territories.

P.2 Applicability

a. This NASA Interim Directive (NID) is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory (JPL) (a Federally Funded Research and Development Center (FFRDC)), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NID covers all NASA-issued IT devices, such as laptops, tablets, USB storage devices, cell phones, and smartphones, that store, process, transmit, or receive NASA information, when such devices are used or carried on international travel. This

directive covers any and all nonpublic NASA information regardless of format and medium of storage, transport, and use. This directive also covers downloads of information and information created during international travel.

c. This policy applies to all NASA personnel (i.e. all persons who have an active identity in NASA's Identity Management and Account Exchange (IdMAX) system) and who are travelling

d. outside of the U.S. and territories while performing any of the following: carrying or using NASA IT resources; carrying NASA Sensitive But Unclassified (SBU) information; using a NASA IT account; or accessing NASA IT resources located in the U.S. or its territories; or visits to U.S. facilities that are under the control of non-U.S. entities. Policies for the management of classified information are included in separate policies.

e. Where noted, this policy applies to NASA personnel who are located outside of the U.S. and territories as a result of a permanent change of station.

f. Direct travel to and from and within U.S. territories and commonwealths is not considered international travel.

g. This policy also applies to visits and meetings to facilities that are owned by or under the control of non-U.S. entities, even when the facilities are within the United States and territories.

h. In this directive, all mandatory actions (i.e., requirements) are denoted by a statement containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

i. Personal device management policies, including bring your own device (BYOD), are described in a separate policy.

j. In this directive, all document citations are assumed to be the latest version, unless otherwise noted.

P.3 Authority

a. Information Technology Management, 40 U.S.C. §11101 et seq.

b. Federal Information Security Management Act (FISMA) of 2014, 44 U.S.C. §3501-3549.

c. Executive Order (E.O.) No. 13011, 61 Fed. Reg. 37657 (July 16, 1996), Federal Information

Technology

d. NPD 2800.1, Managing Information Technology

e. NPD 2810.1, NASA Information Security Policy

f. NID 1600.55, Sensitive But Unclassified (SBU) Information

P.4 Applicable Documents and Forms

NPR 1382.1A, Privacy Procedural Requirements

NPR 1660.1C, NASA Counterintelligence and Counterterrorism

NPR 2190.1, NASA Export Control Program

NAII 2190.1, Export Control Operations Manual

Designated Countries List (see http://oiir.hq.nasa.gov/nasaecp/index.html)

ITS-HBK-2810.07.01, Configuration Management

ITS-HBK 2810.02-2D, Information System Security Assessment and Authorization Process

ITS-HBK-2810.11-01, Media Protection

P.5 Measurement/Verification

Performance measures relative to implementation of this policy are outlined in NASA's Annual
Information Resources Management Strategic Plan, Federal Information Security Management Act Reporting, and Agency E-Government Implementation Plan. Verification is ensured through the NASA CIO internal controls program, the Agency's annual Statement of Assurance process, and the OMB quarterly E-Government scorecard assessment.

P.6 CANCELLATION

None.

Original Signed by

Renee P. Wynn
Chief Information Officer

Chapter 1. Requirements

1.1 Introduction

a. NASA information and information systems, and the accounts that access these systems, need to be protected. This document outlines requirements for fulfilling these responsibilities while employees are outside of the United States and U.S. territories. Travel, work and other activities outside of the U.S. and territories present security challenges that require special attention, additional precautions and modified behavior.

b. This policy separately addresses requirements related to taking and using NASA information on international travel, taking and using NASA IT assets on international travel, and accessing NASA U.S.-based IT resources from locations outside of the U.S. and its territories. Each of these activities presents different risks to NASA's information, information systems, personnel, and mission.

c. The risks relative to the use of NASA information and IT resources may increase depending on the specific destination of international travel. NPR 1660.1C, NASA Counterintelligence and Counterterrorism, contains requirements for all NASA international travelers, and for cleared personnel, to receive threat briefings, as appropriate, for their destination countries.

1.2 Requirements for Use of NASA Information

a. Take NASA internal information on international travel only if the information is required to accomplish official duties. Take only the minimum amount of information required to accomplish NASA duties during travel.

b. Store NASA information that has been designated as SBU (all categories including export controlled International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR)), Personally Identifiable Information (PII), sensitive, or otherwise sensitive unclassified information), only on NASA assets and store strictly in accordance with NID 1600.55, NPR 1382.1A, ITAR, and EAR. Encrypt SBU information on laptops, mobile devices or media while on international travel. This requirement can be satisfied with Data at Rest (DAR) encryption.

c. Prior to travel, prepare and maintain a complete back-up of all NASA information taken on international travel. The back-up will remain in the U.S. The daily workstation provider automated back-up can meet this requirement.

d. Keep a complete and accurate record of all SBU and technical information, including software, taken outside the U.S. This requirement can be satisfied through a pre-travel backup, which can serve as a record of the information. This record will:

(1) Contain sufficient information to identify what SBU and technical data was taken outside the U.S. and U.S. territories.

(2) Be stored in a U.S. location where the record can be easily retrieved in the event of tampering, theft, loss or disclosure of the NASA information during international travel.

e. For all export controlled information, hardware and software, traveling NASA personnel shall comply with NASA export control and travel requirements (NPR 9700.1, NPR 2190.1, NASA Advisory Implementing Instruction (NAII) 2190.1) authorizing the transport of information and IT prior to international travel.

1.3 Requirements for Use of NASA Information Technology

a. Only IT assets that meet the standards and conditions to store, process, transmit, and access NASA information are be authorized for use on international travel. These standards are documented in ITS-HBK-2810.07.01, Configuration Management.

b. Users shall take NASA assets on international travel only if those NASA assets are required to accomplish the job duties to be performed during the travel.

c. Users shall take NASA IT assets or IT assets that process NASA SBU information or use NASA accounts on international travel only when authorized by the Center Chief Information Officer (CIO) or designee.

(1) Users shall ensure that any NASA IT assets which are taken outside of the U.S. and territories (with authorization) are configured in accordance to the NASA security configuration baseline ITS-HBK 2810.07.01.

(2) The only exception is IT assets, such as NASA authorized loaner laptops, loaner tablets or loaner smartphones, which are specifically designated and configured for NASA use while on international travel.

(3) Users shall ensure that all NASA IT assets and any IT assets containing NASA information remain in your possession or are appropriately safeguarded while outside the U.S. and territories (unless there is a specific record of the authority to export per NPD 2190.1).

d. Users shall report any loss, damage, or tampering of NASA IT assets or any IT assets containing NASA information immediately to the NASA Security Operations Center (SOC) (soc@nasa.gov, 877-627-2732).

e. Upon return from international travel, users shall not connect NASA IT assets to NASA internal networks until those assets can be shown to meet the standard recommended by the cognizant Center Information Security Officer (CISO). Contact your CISO for more information regarding the standard scanning process for your Center.

f. Only authorized NASA users are permitted to use NASA managed or owned IT devices, per ITS-HBK-2810.11-01.

g. Users shall keep a complete and accurate record of all NASA hardware taken outside the U.S. The record will:

(1) Contain sufficient information to identify what NASA hardware was taken outside the U.S.
and U.S. territories.

(2) Be stored in a U.S. location where the record can be easily retrieved in case of a theft or loss of the NASA hardware.

h. Users shall comply with NPR 2190.1 and NAII 2190.1, Export Control Policies and Procedures, to record authorizing use of NASA hardware or data outside the U.S. prior to leaving the U.S. or U.S. territories.

1.4 Requirements for Accessing NASA Networks and Information Systems

a. Users shall not access, from outside the U.S. and its territories, any NASA systems, networks, and data not intended for access by the general public without prior written authorization from the Center CIO or designee.

(1) This includes systems where a NASA account is required for access to the resource.

(2) The only exceptions to this requirement are:

i. Access to NASA's Virtual Private Network(s) from a NASA IT asset which has been authorized for international travel.

ii. Direct access to the NASA enterprise email system from an IT asset which has been authorized for international travel and for this direct access.

iii. Access to systems, networks, and data specifically intended for external access by the general public (e.g., publicly accessible web sites).

iv. Access to NASA systems intended for use by national and international authenticated users (including users located in foreign countries) performing NASA-related work (e.g., users of NASA supercomputers).

v. Access to systems established for international collaboration and/or international access, where an Authorization to Operate (ATO) has been granted, pursuant to NASA's Security Accreditation and Authorization (SA&A) process, which includes assessment and management of risks related to this access. (Refer to ITS-HBK 2810.02-2D, Information System Security Assessment and Authorization Process).

b. Outside the U.S. and its territories, users shall only access protected or sensitive NASA systems, networks, and data from a NASA asset. Do not use unauthorized IT assets, such as a public or shared computer or personal devices, to access systems or information not intended for external access by the general public.

Chapter 2. Roles and Responsibilities

2.1 Roles and Responsibilities a. The NASA CIO shall:

(1) Maintain and update this policy.

(2) Establish and maintain a NASA Access Management System module for reporting international travel plans.

b. The NASA Senior Agency Information Security Official (SAISO) shall:

(1) Develop and disseminate guidance to NASA international travelers and other NASA employees that study, work, or conduct other activities abroad.

(2) Develop and disseminate the standards and conditions that must be met for IT to be authorized for use on international travel.

c. Center CIOs, or their designees, shall:

(1) Review and process requests to authorize use of NASA equipment during international travel.

(2) Ensure that loaner assets are available and are properly configured for NASA use while on international travel.

d. Center CISOs, or their desig

nees, shall:

(1) For any upcoming approved travel, contact the traveler to make sure the traveler is meeting IT security requirements.

(2) Review NASA IT assets returning from international travel and provide authorization for reconnecting those NASA IT assets to internal NASA networks. Ensure any necessary mitigation actions are taken prior to re-connection of the NASA IT assets to non-public NASA networks. e. NASA personnel shall:

(1) Comply with all requirements in this document.

(2) Complete the international travel module in the NASA Access Management System (NAMS) 72 hours or more prior to departure.

(3) Take only the information which will be needed for NASA work during travel.

(4) Not access or transport SBU information unless access is required for the performance of duties while on travel, and if required, only using authorized IT assets while on international travel.

(5) Prior to the departure date, back up data and leave a copy in a secure U.S. location.

(6) Encrypt all SBU information (in addition to Data at Rest (DAR) encryption).

(7) Be aware that their belongings may be searched multiple times and electronic media copied.

(8) Report loss, damage, or tampering of NASA IT assets, sensitive unclassified information, and any IT assets containing NASA information to the SOC immediately upon discovery, whether potential or confirmed.

(9) Comply with NASA policy regarding access to NASA networks and information systems.

(10) Comply with other travel policies, including export control (ITAR/EAR).

(11) Keep a complete and accurate record of all NASA hardware taken outside the U.S.

(12) Keep a complete and accurate record of all SBU and technical information, including software, taken outside of the U.S.

f. Center Foreign Travel Coordinators shall:

(1) Identify applicable policy and travel guidance.

(2) Include an overview of this policy in informational materials and training.

(3) Update and maintain travel form templates and systems to reflect the requirements of this policy.

g. The NASA SOC shall:

(1) Receive and collect NAMS notifications about current and upcoming international travel from all NASA personnel.

(2) Maintain NAMS information in a secure repository accessible to Center CISOs, Center Incident Response Teams, and other authorized NASA personnel who require NAMS information.

Appendix A: Definitions

Information Technology -- IT is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency. (1) Hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other. (2) Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: i) requires the use of such equipment; or ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

NASA Asset - A system, object, person, or any combination thereof, owned by NASA, that has importance or value: including facilities, property, information records, data, information technology systems, and applications (NPR 2841.1, Identity Credential and Access Management).

NASA Information – NASA information is defined as any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for or is under the control of NASA.

Non-Public Information – NASA non-public information includes all known categories of and information otherwise assessed as Sensitive But Unclassified (SBU) information and classified information.

Appendix B: Acronyms

ATO	Authorization to Operate
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAR	Data at Rest
E.O.	Executive Order
EAR	Export Administration Regulations
FISMA	Federal Information Security Management Act of 2014
HBK	Handbook
IdMAX	Identify Management and Account Exchange
IT	Information Technology
ITAR	International Traffic in Arms Regulations
NAII	NASA Advisory Implementing Instruction
NAMS	NASA Access Management System
NASA	National Aeronautics and Space Administration
NID	NASA Interim Directive
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement

PCS	Permanent Change of Station
PII	Personally Identifiable Information
SA&A	Security Accreditation and Authorization
SAISO	Senior Agency Information Security Officer
SBU	Sensitive But Unclassified
SOC	Security Operations Center
U.S.C.	United States Code
USB	Universal Serial Bus

Appendix C: References

The Privacy Act of 1974, 5 U.S.C. §552a

Clinger-Cohen Act of 1996, 40 U.S.C. §1401 et seq. (Public Law 104-106, Division E)

OMB Circular No. A-123, Management's Responsibility for Internal Control (12/21/2004)

OMB Circular No. A-130, Management of Federal Information Resources (11/28/2000)

NPD 1382.17I, NASA Privacy Policy

NPD 2190.1, NASA Export Control Program

NPD 2200.2C, Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information

NPD 2810.1, NASA Information Security Policy

NPR 1382.1A, Privacy Procedural Requirements

NPR 1600.1, NASA Security Program Procedural Requirements

NPR 1660.1C, NASA Counterintelligence and Counterterrorism

NPR 9700.1, Travel

NID 1600.55, Sensitive But Unclassified (SBU) Information

NASA Agency Memo, “Protection of Sensitive Agency Information,” April 3, 2012.

NASA CIO Memo, “Minimum Security Requirements for Personal Mobile Devices,” August 27, 2013